# Rappel d'arithmétique : Anneaux modulo $N$

A. Dragut Univ. Aix-Marseille
Cours de cryptographie Chapitre II

**Definition.** *Deux entiers $a$ et $b$ sont dits congrus modulo $N$, où $N \geq 2$ est un entier si leur différence est divisible par $N$, c.à-d. qu'il existe un entier $k$ tel que $a - b = kN$. On note $a \equiv b \pmod N$ et on dit que $a$ est équivalent/congru à $b$ modulo $N$.*

Souvent, par commodité, $\equiv$ est remplacé par $=$ même si cela reste faux dans l'absolu .

**Notation.** *$\mathbb{Z}_N$ ou $\mathbb{Z}/N\mathbb{Z} = \{0, 1, 2, ..., N-1\}$ l'ensemble des restes modulo $N$ (c.à-d. à la division par $N$)*

On définie sur $\mathbb{Z}_N$ des opérations d'addition et de multiplication analogues à celles définies sur les entiers :

**Addition :** à deux restes $a$ et $b$, on associe le reste de la somme $a + b$ à la division par $N$ et on note "$(a + b) \pmod N$". Ainsi modulo 7, on écrira $3 + 2 = 5$ mais $4 + 4 = 1$ car la somme de 4 et 4 a pour reste 1 modulo 7.

**Multiplication :** à deux restes $a$ et $b$, on associe le reste de produit $ab$ à la division par $N$ et on note "$(ab) \pmod N$". Ainsi modulo 7, on écrira $2 \cdot 2 = 4$ mais $3 \cdot 3 = 2$ car le produit de 3 et 3 a pour reste 2 modulo 7.

Pour ces operations dans $\mathbb{Z}/N\mathbb{Z}$, il est naturel de s'intéresser à l'existence de l'opposé et de l'inverse modulo $N$, ainsi qu'aux puissances successives.

**Definition.** *Un anneau unitaire est un triplet $(A, +, \cdot)$ tel que :*

1. *$A$ est un ensemble*
2. *la loi $+$ est une loi de composition interne telle que $(A, +)$ soit un groupe commutatif/abélien, c.à-d.*
   - *la loi $+$ est associative : $a + (b + c) = (a + b) + c$ ;*
   - *$A$ un élément neutre pour la loi $+$, noté $0$ : $a + 0 = 0 + a = a$ ;*
   - *tout élément $a$ de $A$ a un opposé, noté $-a$ : $a + (-a) = (-a) + a = 0$ ;*
   - *la loi $+$ est commutative : $(a + b = b + a)$ ;*
3. *$\cdot$ est une loi de composition interne associative : $(a \cdot b) \cdot c = a \cdot (b \cdot c) = a \cdot b \cdot c$ ;*
4. *la loi $\cdot$ est une loi de composition interne distributive par rapport à $+$ :*
   - *$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ (Distributivité à gauche) ;*
   - *$(a + b) \cdot c = (a \cdot c) + (b \cdot c)$ (Distributivité à droite) ;*
5. *$A$ a un élément neutre pour la loi $\cdot$, noté $1$ : $a \cdot 1 = 1 \cdot a = a$ ;*
6. *$A$ est un anneau commutatif si sa seconde loi $\cdot$ est aussi commutative : $(a \cdot b = b \cdot a)$ ;*
7. *un élément $a \in A$ est inversible si existe $b \in A$ et $a \cdot b = b \cdot a = 1$. On note $b = a^{-1} = 1/a$.*

**Proposition.** $(\mathbb{Z}/N\mathbb{Z}, +, \cdot)$ ***est un anneau unitaire commutatif.***

**Notation.** *On note avec* $(\mathbb{Z}/N\mathbb{Z})^*$ *ou* $\mathbb{Z}_N^*$ *le sous-groupe multiplicatif du* $(\mathbb{Z}/N\mathbb{Z}, +, \cdot)$ *formé par ses éléments inversibles.*

## 2.1 Algorithme d'Euclide étendu.

**Lemme 1.** *Soient* $a$, $b$,$q$ *et* $r > 0$ *avec* $a = q \cdot b + r$. *Alors* $\text{pgcd}(a, b) = \text{pgcd}(r, b)$.

On utilise ce lemme pour calculer le plus grand diviseur commun des entiers $j$ et $k$. L'algorithme est récursif et réduit les entiers jusqu'à ce que le reste devienne nul. Il est convenable de supposer que les deux entiers sont positifs et que $b \leq a$.

### Algorithme du pgcd étendu

On modifie maintenant l'algorithme pour qu'il renvoie les entiers $x$ et $y$ pour lesquels $\text{pgcd}(a, b) = x \cdot a + y \cdot b$. Pour cela, il suffit d'éliminer successivement les restes des divisions et de remonter les calcules des divisions euclidiennes.

**Exemple.** *Trouver les coefficients Bachet-Bézout pour* 255 *et* 141 *en utilisant l'algorithme d'Euclide étendu.*

$$\begin{array}{llrcrcrcr}
(1) & 255 & = & 1 & \times & 141 & + & \boxed{114} \\
(2) & 141 & = & 1 & \times & 114 & + & \boxed{27} \\
(3) & 114 & = & 4 & \times & 27 & + & \boxed{6} \\
(4) & 27 & = & 4 & \times & 6 & + & \boxed{3} \\
 & 6 & = & 2 & \times & 3 & + & 0
\end{array}$$

Maintenant on élimine les restes :

$$\begin{array}{rcrcrcl}
4 & = & 27 & - & 4 & \times & \boxed{6} \\
 & = & \boxed{27} & - & 4 & \times & (114 - 4 \times \boxed{27}) \\
 & = & -4 \times 114 & + & 17 & \times & \boxed{27} \\
 & = & -4 \times \boxed{114} & + & 17 & \times & (141 - 1 \times \boxed{114}) \\
 & = & 17 \times 141 & - & 21 & \times & \boxed{114}) \\
 & = & 17 \times 141 & - & 21 & \times & (255 - 1 \times 141) \\
 & = & 38 \times 141 & - & 21 & \times & 255
\end{array}$$

Les coefficients Bachet-Bézout sont 38 et $-21$.

## 2.2 Le sous-groupe $((\mathbb{Z}/N\mathbb{Z})^*, \cdot)$. Calcul de l'inverse $\pmod N$

### 2.2.1 Calcul de l'inverse modulaire avec Euclide étendu

**Definition.** *Deux entiers $a$ et $b$ sont* premiers entre eux *(ou bien $a$ est dit* premier avec $b$*) s'il n'ont pas de diviseurs premiers communs, ou bien, de manière équivalente, si* $\text{pgcd}(a, b) = 1$.

**Théorème.** [**Bachet-Bézout**] *Soient deux entiers non-nuls $u$ et $v$. Si* $\text{pgcd}(u, v)$ *est le PGCD de $u$ et de $v$, alors il existe deux entiers $x$ et $y$ tels que $x \cdot u + y \cdot v = \text{pgcd}(u, v)$ En particulier, deux entiers sont relativement premiers entre eux si et seulement s'il existe deux entiers $x$ et $y$ tels que $x \cdot u + y \cdot v = 1$*

**Corollaire.** *Soit $a \in \mathbb{Z}/N\mathbb{Z}$ tel que $a$ et $N$ sont premiers entre eux, alors $a$ a un inverse modulo $N$.*

**Preuve.** *Donc $a \in (\mathbb{Z}_N^*$ le sous ensemble de $\mathbb{Z}/N\mathbb{Z}$ contenant les éléments premiers avec $N$, c.à-d. $\{a \in \mathbb{Z}/N\mathbb{Z} \,|\, \text{pgcd}(a, N) = 1\}$. Parce que $\text{pgcd}(a, N) = 1$, l'algorithme étendu d'Euclide renvoie les entiers $U$ et $V$ tels que $Ua + VN = 1$. En appliquant le modulo $N$ à cette équation, on élimine le multiple de $N$. On obtient donc $Ua \equiv 1 \pmod N$. Selon la definition de l'inverse modulo $N$ (c.à-d. $U^{-1} \cdot U \equiv 1 \pmod N$), l'entier $U$ est l'inverse de $a$.*

On peut utiliser l'algorithme étendu d'Euclide pour calculer l'inverse multiplicatif de $a$ tel que $pgcd(a, N) = 1$.

**Exemple.** $9^{-1} \pmod{16}$

$16 = 1 \cdot 9 + 7$;
$9 = 1 \cdot 7 + 2$;
$7 = 3 \cdot 2 + 1$;
$2 = 2 \cdot 1 + 0$ donc $\text{pgcd}(16, 9) = 1$.

En écrivant les restes nous avons $7 = 16 - 19; 2 = 9 - 17$. En commençant du dernier reste non-nul nous avons
$1 = 7 - 3 \cdot 2 = 7 - 3 \cdot (9 - 1 \cdot 7) = -3 \cdot 9 + 4 \cdot 7 = -3 \cdot 9 + 4 \cdot (16 - 1 \cdot 9)$.
$1 = 4 \cdot 16 - 7 \cdot 9$ et donc $9^{-1} = -7 = 9 \pmod{16}$.

Une autre variante de calculer l'inverse multiplicatif modulo $N$ avec un $N$ petit est d'utiliser directement le théorème Bachet-Bézout pour deux nombres qui sont premiers entre eux. Si $x = 9^{-1}$, alors $9 \cdot x \equiv 1 \pmod{16}$. Donc on écrit : $9 \cdot x = 16 \cdot k + 1$ et on itère sur $k = 1, 2, ..., 16 - 1$ pour trouver un multiple de 9. Pour $k = 1$ on obtient 17, après 33, après 49, après 65, après 81 qui est un multiple de 9. Donc $9^{-1} = 9 \pmod{16}$.

### 2.2.2 Calcul de l'inverse modulaire avec Euler/Fermat

**Corollaire.** *Si $p$ est premier, alors chaque entier non-nul $a \in \mathbb{Z}/p\mathbb{Z}$ a un inverse. On note avec $\mathbb{F}_p^* = (\mathbb{Z}/p\mathbb{Z})^* = 1, 2, ..., p - 1$*

**Preuve.** *En supposant* $\text{pgcd}(e, N) = 1$*, l'algorithme étendu xPGCD renvoie les entiers* $U$ *et* $V$ *tels que* $Ue + VN = 1$*. En appliquant le modulo* $N$ *cette équation, on obtient les entiers* $Ue \equiv 1 \pmod{N}$*. Donc selon la definition de l'inverse modulo* $N$*, l'entier* $U$ *est l'inverse de* $e$*.*

**Corollaire.** *Si* $p$ *est premier* $\mathbb{F}_p^* = (\mathbb{Z}/p\mathbb{Z})^* = 1, 2, ..., p-1$ *est le sous-groupe du corps* $\mathbb{Z}/p\mathbb{Z}$ *par rapport à la loi* $\cdot$*.*

**Definition.** *Soit l'anneau* $\mathbb{Z}/N\mathbb{Z}$ *et soit* $(\mathbb{Z}/N\mathbb{Z})^* = \{a \in \mathbb{Z}/N\mathbb{Z} \,|\, \text{pgcd}(a, N) = 1\}$ *son sous-groupe contenant les entiers qui sont premiers avec* $N$*. On appelle fonction indicatrice d'Euler* $\phi(N)$ *la cardinalité de* $(\mathbb{Z}/N\mathbb{Z})^*$*, c'est-à-dire* $\phi(N) = |(\mathbb{Z}/N\mathbb{Z})^*|$*.*

Les propriétés de $\phi(N)$ sont :

1. Si $p$ est premier, alors $\phi(p) = p - 1$
2. Plus généralement, si $p$ est premier et $k \geq 1$, alors
$$\phi(p^k) = p^k - p^{k-1} = (p-1)p^{k-1}$$
3. Si $\text{pgcd}(p, q) = 1$, alors $\phi(pq) = \phi(p)\phi(q)$.
4. Si $N = p_1^{e_1} \cdots p_k^{e_k}$, où $p_1, \ldots, p_k$ sont des nombres premiers tous distincts, et $e_1, \ldots, e_k$ sont des entiers positifs. Alors
$$\phi(N) = (p_1 - 1) \cdot p_1^{e_1 - 1} \cdots (p_k - 1) \cdot p_k^{e_k - 1}$$

**Exemple.** *Calculer* $\phi(126)$ *en utilisant la factorisation de* $N = 2 \cdot 3^2 \cdot 7$*.*

$$\begin{aligned} \phi(126) &= \phi(2) \cdot \phi(3^2) \cdot \phi(7) \\ &= (2-1) \cdot (3-1)(3^{2-1}) \cdot (7-1) \\ &= 1 \cdot 2 \cdot 3 \cdot 6 = 36 \end{aligned}$$

**Théorème** (Euler)**.** $x^{\phi(N)} \equiv 1 \pmod{N}$ *pour tout* $x \in (\mathbb{Z}/N\mathbb{Z})^*$*, c.à-d.* $pgcd(a, N) = 1$*.*

La preuve est immediate seulement pour ceux familiers avec la théorie de groupes. On applique le Th. de Lagrange pour $(\mathbb{Z}/N\mathbb{Z})^*$ et pour le sous-groupe cyclique généré par $x$.

Sinon on peut se contanter de prouver séparément le cas spécial d'une version réduite

**Théorème** (petit théorème du Fermat version réduite)**.** $x^{p-1} \equiv 1 \pmod{p}$ *pour tout* $x \in (\mathbb{Z}/p\mathbb{Z})^*$*,* $1 \leq x \leq p-1$*, où* $p$ *est premier.*

**Preuve.** *Ébauche :*

*On prend les nombres* $x, 2x, ..., (p-1)x$. *Nous avons que* $ix \equiv jx$ *si et seulement si* $(i-j)x$ *est divisible par* $p$. *Mais* $pgcd(x,p) = 1$ *et* $0 \leq (i-j) < p-1$ *et donc il ne peut pas être un vrai multiple de* $p$. *Donc* $i - j = 0$. *Donc ils sont* $p-1$ *nombres distinctes modulo* $p$. *Mais dans le groupe* $(\mathbb{Z}/p\mathbb{Z})^*$ *il n'y a que* $p-1$ *éléments distincts au total. Donc* $x \cdot 2x \cdot ... \cdot (p-1)x = (p-1)!$. *Alors,* $(p-1)! \cdot x^(p-1) = (p-1)!$. *En simplifiant on prouve le résultat.*

**Théorème** (petit théorème du Fermat)**.** *Soit* $p$ *un nombre premier et* $x$ *un entier arbitraire. Alors* $x^{p-1} \equiv 1 \pmod{p}$ *ou équivalent* $x^p \equiv x \pmod{p}$..

**Preuve.** *L' hypothèse du théorème est vérifie pour* $x = 0$ *et* $x = 1$. *Supposons par induction que hypothèse est vraie pour un nombre entier* $x$ *et vérifions la pour* $x+1$. *Mais* $(x+1)^p \equiv x^p + 1 \equiv x + 1 \pmod{p}$ *parce que*

$$(x+y)^p = \sum_{k=0}^{p} \frac{p!}{k!\,(p-k)!} x^{p-k} y^k.$$

*Donc le pas d'induction est vérifie.*

*Pour* $p = 2$ *hypothèse est vraie aussi pour tout entier négatif. Si* $p$ *est impaire et* $x^p \equiv x \pmod{p}$ *nous avons* $(-x)^p \equiv x^p \equiv -x \pmod{p}$.

**Exemple.** *Calculer* $9^{-5} \pmod{19}$ *(pour ElGamal)*

L'entier 19 est premier. On sait que $9^{18} \equiv 1 \pmod{19}$. Mais $1 \equiv 9^{18} = 9^{13} \cdot 9^5 \pmod{19}$. Donc selon la définition de l'inverse modulo $p = 19$ nous avons que $9^{-5} \equiv 9^{13} \equiv 3 \pmod{19}$

## 2.3 Le théorème chinois des restes

**Théorème.** *(Le théorème chinois des restes)Si* $n_1, \cdots, n_k$ *sont deux à deux premiers entre eux alors, en notant* $n$ *le produit des* $n_i$, *la fonction*

$$\begin{array}{rccc} \phi: & \mathbb{Z}/N\mathbb{Z} & \longrightarrow & \mathbb{Z}/p_1\mathbb{Z} \times \cdots \times \mathbb{Z}/p_k\mathbb{Z} \\ & \alpha & \longmapsto & (\alpha \pmod{p_1}, \ldots, \alpha \pmod{p_k}) \end{array}$$

*est un isomorphisme d'anneaux. Dans le cas où les* $p_i$ *ne sont pas premiers entre eux,* $N$ *est leur ppcm et le morphisme ci-dessus n'est qu'injectif.*

**Théorème.** ***(Le théorème chinois des restes version des congruences)*** *Soient* $p_1, \cdots, p_k$ *sont deux à deux premiers entre eux. On note avec* $N$ *le produit des* $p_i$. *Soient les entiers arbitrairement choisis* $\alpha_1, \cdots, \alpha_k$. *Alors il existe un entier* $z$, *unique modulo* $N$, *tel que*

$$\begin{array}{c} z \equiv \alpha_1 \pmod{p_1} \\ \cdots \\ z \equiv \alpha_k \pmod{p_k} \end{array}$$

**Preuve.** *Parce que pour chaque $i$, les entiers $p_i$ et $\frac{N}{p_i} = p_1 \dots p_{i-1} p_{i+1} \dots p_k$ sont premiers entre eux, le théorème de Bachet-Bézout s'applique et il existe les entiers $u_i$, et $v_i$, tels que $u_i p_i + v_i \frac{N}{p_i} = 1$.*

*Pour $e_i = v_i \cdot \frac{N}{p_i}$ nous avons pour chaque $i$*

$$\begin{aligned} e_i &\equiv 1 \pmod{p_i} \\ e_i &\equiv 0 \pmod{p_j} \, pour j \neq i \end{aligned}$$

*Une solution $z$ du système de congruences est $z = \sum_{i=1}^{k} \alpha_i e_i$, où $e_i = v_i \cdot \frac{n}{n_i}$ et $v_i$ sont les entiers du le théorème de Bachet-Bézout.*

*Soit $\overline{z}$ une autre solution du système de congruences. Nous avons $\overline{z} \equiv z \pmod{p_i}$ pour chaque $i$. Donc il existe l'entier $t$ tel que $\overline{z} - z = t \cdot p_1$. Parce que pour chaque $i$, les entiers $p_i$ sont premiers entre eux $t$ est divisible par $p_j$ pour chaque $j \neq i$, donc $\overline{z} - z$ est divisible par $N = p_1 \dots p_k$. $\overline{z} \equiv z \pmod{N}$*

## 2.4 Groupe cyclique fini. Résultats pour ElGamal

**Definition.** *Un groupe cyclique $G$, est un groupe dans lequel il existe un élément $g$ tel que tout élément du groupe puisse s'exprimer sous forme d'un multiple/puissance de $g$, cet élément $g$ est appelé générateur du groupe et on note $G =< g >$.*

**En notation additive** : $(G, +)$ $[n]g$
**En notation multiplicative** : $(G, \cdot)$ $g^n$

**Definition.** *Soit $G$ un groupe et $g \in G$, alors le groupe sous-groupe $H$ généré par $g$, noté $H =< g >$, est le plus petit sous-groupe de $G$ contenant $g$.*

**Definition.** *L'ordre d'un élément $g$ d'un groupe $G$ est noté $ordre(g)$ ou $o(g)$. Si l'ordre est fini, il est le plus petit entier $m > 0$ tel que*
- *En notation additive : $mg = 0$*
- *En notation multiplicative : $g^m = 1$*

***On peut dire que si l'ordre de $g$ est fini*** $ordre(g) = |H| = | < g > |$ ***la cardinalité sous-groupe $H =< g >$ généré par $g$.***

Pour un groupe $G$ fini, la cardinalité sous-groupe $H =< g > \subset G$ généré par $g$ est un nombre fini n'importe quel élément $g$ multiplié par lui-même de manière répétée doit être dans le groupe $G$. Mais le groupe $G$ a un nombre fini d'éléments, alors les puissances de $g$ finissent par se répéter.

**Exemple.** *Pour $x = 5 \in (\mathbb{Z}/26\mathbb{Z})^*$ : $5, 25, 21, 1, 5, 25, 21, 1, \ldots$*

**Exemple.** *Trouver l'ordre de l'élément 2 dans*
- *$F_{11}^* = (\mathbb{Z}/11\mathbb{Z})^* = \{1, 2, ..., 10\}$ le groupe multiplicatif de restes modulo 11*
- *$F_{17}^* = (\mathbb{Z}/17\mathbb{Z})^* = \{1, 2, ..., 16\}$ le groupe multiplicatif de restes modulo 17*

Dans $\mathbb{F}_{11}^*$ nous avons $2^0 = 1$, $2^1 = 2$, $2^2 = 4$, $2^3 = 8$, $2^4 \equiv 5$, $2^5 \equiv 10$, $2^6 \equiv 9$, $2^7 \equiv 7$, $2^8 \equiv 3$, $2^9 \equiv 6$. Mais $2^{10} \equiv 1$ et on commence à répéter les éléments.

Donc $ordre(2) = 10$ et il génère tout le groupe $G$.

Dans $\mathbb{F}_{17}^*$ nous avons $2^0 = 1$, $2^1 = 2$, $2^2 = 4$, $2^3 = 8$,$2^4 = 16$, $2^5 \equiv 15$, $2^6 \equiv 13$, $2^7 \equiv 9$. Mais $2^8 \equiv 1$ et on commence à répéter les éléments. Donc 2 n'est pas un générateur pour $\mathbb{F}_{17}^*$. Il génére que le sous-groupe $H =< 2 >= \{1, 2, 4, 8, 9, 13, 15, 16\}$ et son ordre est la cardinalité de ce sous-groupe, donc 8.

Pour $p$ premier la structure du groupe multiplicatif de $\mathbb{Z}/p\mathbb{Z}$ est celle d'un groupe abelién fini cyclique d'ordre $\phi(p) = p - 1$.

**Théorème. [racine primitive/générateur]** *Soit $p$ premier. Alors il existe $g \in \mathbb{F}_p^*$ tel que $(\mathbb{F}_p^*, \cdot) = \{1, g, \ldots, g^{p-2}\}$. L'ordre de $g$ est $ord(g) = |\mathbb{F}_p^*| = p - 1$.*

**Corollaire.** *(du Th. Lagrange) Soit $p$ un entier premier. Soit $H =< g > \subseteq (\mathbb{F}_p^*, \cdot)$ et $ord(g) = |H| = q$. Alors $q/(p-1)$.*

**Exemple.** $\mathbb{F}_{11}^*$ *:* $2^0 = 1$, $2^1 = 2$, $2^2 = 4$, $2^3 = 8$, $2^4 \equiv 5$, $2^5 \equiv 10$, $2^6 \equiv 9$, $2^7 \equiv 7$, $2^8 \equiv 3$, $2^9 \equiv 6$, $2^{10} \equiv 1$ *, mais* 2 *n'est pas un générateur pour* $\mathbb{F}_{17}^*$.

**Exemple.** *Le groupe multiplicatif* $\mathbb{F}_{11}^*$ *a la cardinalité* 10*, donc les ordres des elements de* $\mathbb{Z}_{11}$ *sont :* $1, 2, 5, 10$.

Par exemple $< 3 >= 1, 3, 9, 5, 4$ est le sous-groupe d'ordre 5 du groupe multiplicatif $\mathbb{F}_{11}^*$.